Automatic DNSSEC Zone Signing Key rollover explained

Updated on 27 Sep 2018 | 5 minutes to read | Contributors

This article is derived from a blog post on our website that introduced the ***9.7.2 changes in automatic in-server key rollover (https://www.isc.org/blogs/bind-9-7-2-and-automatic-dnssec-signing)****.*

BIND 9.7.0 introduced automatic in-server signature refreshing and automatic key rollover. This allows BIND, if provided with the DNSSEC private key files, to sign records as they are added to the zone, or as the signatures need to be refreshed. This refresh happens periodically to spread out the load on the server and to even out zone transfer load.

From BIND 9.7.2 (and all current production versions of BIND 9.7 and newer), when a new Zone Signing Key (ZSK) is being rolled to, BIND will manage a gradual transition of signatures from the old key to the new key.

Description of Key Timers

Before we dig too deeply into how a gradual key roll may occur, we need to describe the internal state BIND 9 maintains for a particular key. This is a description of how a Zone Signing Key (ZSK) is tracked within BIND 9.7. A similar method is used for Key Signing Keys but is not documented here.

In BIND 9.6, external tools were used to re-sign the zone, namely **dnssec-signzone**. The keys were managed externally to the server process, usually manually. Key management was performed by controlling which private keys the command line tool had access to when signing was performed. In BIND 9.7, management of keys has been moved into the server.

A ZSK changes states using defined points in time. These states are: *Created*, *Publish*, *Activate*, *Inactive*, and *Delete*. The private key file itself maintains these timers and they are set upon key creation or through a command line tool. Once specified, these timers trigger the necessary state changes. The key states are used by the server for key selection when signing and for determining which keys